



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/672,796

09/26/2003

Andrew Morgan

TRAN-P162

9469

7590 07/17/2008
WAGNER, MURABITO & HAO LLP
Third Floor
Two North Market Street
San Jose, CA 95113

EXAMINER

PICH, PONNOREAY

ART UNIT

PAPER NUMBER

2135

MAIL DATE

DELIVERY MODE

07/17/2008

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/672,796	Applicant(s) MORGAN ET AL.	
	Examiner PONNOREAY PICH	Art Unit 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 26 March 2008.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-26 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-26 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Claims 1-26 are pending.

Response to Arguments

Applicant's arguments submitted on 3/26/08 were fully considered, but were not persuasive.

Applicant argues that Easter and Chorley fails to teach "wherein said digital secret is stored only within said processor". The examiner respectfully disagrees. It would appear that applicant has only considered the teachings of the references separately rather than consider what the teachings of both references together would have suggested to a person of ordinary skill in the art at the time applicant's invention was made. One cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). Easter, as applicant clearly recognizes, teaches storage of keys only within an IC. In Easter's case, the IC is outside the processor as seen in Figure 2. However, Easter's IC is meant to be incorporated in to circuitry (col 6, lines 14-22). Further, Chorley additionally teaches that in the prior art, one known software protection method attempted to protect software by only performing decryption of software within a processor (col 1, lines 34-39). In this manner, intruders are prevented from having access to the software and the keys used to decrypt the software. This implies that in the prior art software protection scheme disclosed by Chorley, the keys used to decrypt the software along with the decryption engine are only stored in the

processor or are part of the processor. In other words, from Chorley's teachings, it would have been obvious to one of ordinary skill in the art to modify Easter's invention such that rather than have the IC 63 containing the cryptographic engine outside a processor, the IC was integrated as part of the processor. By modifying Easter's invention in the manner discussed, the digital secret in the combination invention is only stored within the processor because the IC has become part of the processor. A processor is a type of circuit, thus the combination proposed by the Office would go along with what Easter wants since the IC would then be incorporated into circuitry as discussed above.

Applicant argues Easter teaches away from storing a digital secret within the processor since in this invention, the key is stored outside the processor. The examiner respectfully disagrees. Easter does not in any way teach that it would be undesirable to only store a key inside a processor or incorporate the IC as part of the processor as the examiner is proposing based on Chorley's teachings. Applicant has not pointed to any specific teachings of Easter where he states that it would be undesirable to store a key inside the processor. Easter's IC is for incorporation into further circuitry (col 6, lines 14-22), thus incorporating the IC into a processor (a type of circuitry) as proposed by the examiner goes along with Easter's teachings rather than teach away from it as applicant is arguing.

Applicant argues that the keys stored in key array 25 are public keys, thus are not digital secrets or secret keys as claimed, thus teaches away from the claimed embodiment. The examiner respectfully disagrees. Using claim 1 as an example, the

Art Unit: 2135

claim recites that the digital secret comprises a secret key and the digital secret is operable for use by the processor for both encryption and decryption. The language of the claim is met because Easter's array stores a private key, a serial number, and a hash value for a corresponding public key (col 5, lines 32-36). A private key as a person of ordinary skill in the art would understand is a secret key because it is not meant to be shared. Thus, even though Easter uses a public key system for his cryptography engine, the language of the claim is met since he stores a digital secret which comprises a private/secret key, serial number, and hash value for a corresponding public key. These digital secret are used for both encryption and decryption of data by the IC 63, which in the proposed combination invention of Easter and Chorley is part of a processor.

Applicant argues that Easter fails to teach "wherein said digital secret and said internal memory are fully integrated within said cryptography engine to facilitate communication without use of a bus" as recited in claims 19 and 26. The examiner respectfully disagrees. IC 63 as disclosed by Easter in Figure 2 can be considered a cryptography engine. IC stands for "integrated circuit" and the key arrays storing the keys which the examiner is considering the digital secret are memory internal to the integrated circuit 63, thus does not use any external bus to facilitate communication with IC 63. Bus 37 is internal to the IC, however, as a person of ordinary skill would understand, even circuits that are integrated have internal buses that allow for communication between the components that make up the integrated circuit. It is impossible to build a cryptography engine which communicates with a memory without

Art Unit: 2135

use of even an internal bus even if the memory and cryptography engine were integrated together as a single integrated circuit. Applicant's argument, which appears to state that even internal buses of an integrated circuit is to be excluded from existing as part of the claimed invention as per the limitation being argued, does not reflect what a person of ordinary skill in the art would have understood applicant's invention to be as disclosed in the specification. A person of ordinary skill in the art would have understood that even if different electronic components were integrated into one integrated circuit, internal buses would still be needed to connect the different components together to allow for transfer of data between those components. The "without use of a bus" as disclosed in the specification and claimed would have been understood by one of ordinary skill in the art as referring to external buses only. Since the key array is integrated into IC 63, no external buses exist to facilitate communication between the key array and IC 63. If applicant is insisting that "without use of a bus" also covers internal buses of an integrated circuit, then the examiner respectfully request under 37 CFR 105 an explanation and proof of how information can be transferred between two different circuit without use of any sort of bus, even internal buses. A bus is just some form of pathway for electrons in a circuit to travel, thus if no buses are used at all, applicant is essentially claiming that it is possible to transport electrons from one place to another without use of any sort of connecting pathway. Applicant's disclosure has not been enabled for such an act and as far as the examiner is aware, science has not advanced to such a point.

Applicant argues that Easter teaches away from the claimed embodiments by teaching that the keys within the key array 25 are public keys instead of digital secrets as claimed. This argument had been raised before and already traversed above. Key array 25 has at least a private key which is a secret key and along with the other data stored within the key array, fits the requirements of the claimed digital secret, thus does not teach away from the claimed invention.

Applicant argues that one of ordinary skill would not be motivated to implement Easter's IC 53 within Chorley's processor since Easter teaches away from such a combination by teaching the components of IC 53 are separate from the CPU 13. The examiner respectfully disagrees. A CPU is a type of circuit and Easter clearly states that IC 63 is for incorporation into circuitry (col 6, lines 14-22).

Applicant states that Chorley teaches that the security of the processor is poor, thus the combination of Easter and Chorley in the claimed fashion would decrease the security of the invention and reveal the key, thus one skilled would not have been motivated to combine Easter and Chorley in the claimed fashion. The examiner respectfully submits that the teachings of the prior art as a whole must be considered. The examiner was not proposing combining Easter's teachings with the teachings of Chorley's invention. The examiner was proposing combining Easter's teachings with what Chorley disclosed was done in the prior art to protect software. Chorley recognizes the shortcomings of what was done in the prior art he discusses and his invention was to overcome those short comings. However, the fact that Chorley discloses that the prior art attempted to secure software by incorporating a cryptography

engine and keys within a processor as the examiner is proposing shows that at the time applicant's invention was made, it would have been obvious to one skilled in the art to combine Easter and the prior art teachings of Chorley in the manner discussed by the Office and for the reasons discussed.

The remaining claims are towards dependency, thus are traversed since the arguments for the independent claims were traversed.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Note that with respect to the current application, a person of ordinary skill in the art is determined to be someone with a BS in Computer Science or Electrical/Computer Engineering (or someone with equivalent industry experience) and is familiar with basic electronic circuit design and basic cryptographic techniques.

Claims 1-3, 5-7, 9-11, 14-15, 18-21, and 26 are rejected under 35 U.S.C. 103(a) as obvious over Easter et al (US 5,563,950) in view of Chorley et al (US 4,634,807).

Claim 1:

Easter discloses:

1. A digital secret comprising a secret key (i.e. the DES secret key) used in a key based cryptographic process (Fig 5; col 4, lines 27-29; and col 8, lines 18-18).
2. A cryptographic engine for performing said key-based cryptographic process internally within said processor (Fig 5, DES engine 21), said cryptographic engine operable to access said digital secret (col 8, lines 18-22 and Fig 5).
3. Internal memory coupled to said cryptographic engine for supporting said key-based cryptographic process (Fig 5, items 25 and 51).

Easter does not explicitly disclose wherein said digital secret is stored only within said processor. However, Easter discloses storing a key only within an integrated circuit (col 5, lines 6-11 and col 6, lines 14-19). Further, Chorley discloses of a well known prior art software protection method where software is stored in an encrypted form in a user's storage and the software is decrypted and run from within a secure processor and intruders are prevented from having access to the software and the keys used to encrypt and decrypt the software (col 1, lines 34-39).

At the time applicant's invention was made, it would have been obvious to one skilled in the art to utilize Easter's teachings within the prior art software protection system disclosed by Chorley. One skilled would do so by only storing the DES encryption key within the IC chip disclosed by Easter and by utilizing the IC chip disclosed by Easter as part of the secure processor disclosed by Chorley to secure software via DES encryption/decryption. One skilled would have been motivated to only

Art Unit: 2135

store the DES encryption key within the IC chip disclosed by Easter because it would prevent unauthorized personnel from accessing the key and the software. Note that this was something that Chorley's prior art invention disclosed that it wanted to do, but Chorley did not discuss how to accomplish this. Incorporation of Easter's teachings of only storing a key within an integrated circuit would accomplish this. Note also that the IC chip disclosed by Easter is meant to be incorporated as part of further circuitry (col 6, lines 14-15), thus it would have been obvious to incorporate Easter's IC chip 53 as part of Chorley's secure processor.

Note also that the prior art software security system disclosed by Chorley is one ready for improvement because he does not discuss what sort of encryption scheme to use, does not discuss the secure processor in detail, and does not discuss how to prevent an intruder from having access to a key. The use of Easter's teachings within the prior art software protection system disclosed by Chorley would do no more than yield the predictable result of a secure processor that secured software using DES and one which has a DES key stored only within the processor to prevent unauthorized parties from gaining access to the software. Applying a known technique to a known device (methods or products) ready for improvement to yield a predictable result is obvious.

Claim 10:

Easter discloses:

1. A secure cryptographic unit (Fig 5, item 53), said cryptographic unit comprising:

- a. A cryptographic engine for performing a key-based cryptographic process (Fig 5, items 57 and 21).
- b. A digital secret exclusively accessible to said cryptographic engine, wherein said digital secret comprises a secret key used in said key-based cryptographic process, and wherein said secret key is operable to be used for both encryption and decryption (col 4, lines 28-29 and col 8, lines 10-22).
- c. Internal memory coupled to said cryptographic engine for supporting said key-based cryptographic process (col 8, lines 10-22 and Fig 5).

Easter does not explicitly disclose wherein said cryptographic unit internally provides secure cryptographic capabilities as a functional unit within said processor and said secret key is exclusively used by said processor. However, Easter discloses that his secure cryptographic unit is meant to be incorporated into circuitry (col 6, lines 15-16). Easter discloses storing a key only within an integrated circuit (col 5, lines 6-11 and col 6, lines 14-19). Further, Chorley discloses of a well known prior art software protection method where software is stored in an encrypted form in a user's storage and the software is decrypted and run from within a secure processor and intruders are prevented from having access to the software and the keys used to encrypt and decrypt the software (col 1, lines 34-39).

At the time applicant's invention was made, it would have been obvious to incorporate Easter's secure cryptographic unit into the secure processor disclosed by

Art Unit: 2135

Chorley so that said cryptographic unit internally provides secure cryptographic capabilities as a functional unit within said processor and said secret key is exclusively used by said processor. The rationale for why it would have been obvious to combine Easter and Chorley's teachings is the same as what was discussed in claim 1.

Claim 21:

Easter discloses:

1. A secure hardware environment providing core processing functionality (Fig 5, item 53), wherein said secure hardware environment comprises:
 - a. A secure cryptography unit (Fig 5, item 21), for providing secure cryptographic capabilities as a functional unit within said secure hardware environment (Fig 5), wherein said secure cryptography unit is operable to facilitate performance of a key-based cryptographic process and wherein said key-based cryptographic process comprises encryption using a digital secret and decryption using said digital secret (col 4, lines 28-29 and col 8, lines 10-22).

Easter does not explicitly disclose said key-based cryptographic process is performed exclusively by said processor. However, Easter discloses that his secure cryptographic unit is meant to be incorporated into circuitry (col 6, lines 15-16). Easter discloses storing a key only within an integrated circuit (col 5, lines 6-11 and col 6, lines 14-19). Further, Chorley discloses of a well known prior art software protection method where software is stored in an encrypted form in a user's storage and the software is

Art Unit: 2135

decrypted and run from within a secure processor and intruders are prevented from having access to the software and the keys used to encrypt and decrypt the software (col 1, lines 34-39).

At the time applicant's invention was made, it would have been obvious to one skilled in the art to utilize Easter's IC circuit 53 in the secure processor disclosed by Chorley. The rationale for why it would have been obvious to combine Easter and Chorley's teachings is the same as what was discussed in claim 1.

Claim 2:

Easter further discloses an internal bus for facilitating secure communication between said cryptography engine, said digital secret, and said internal memory within said processor (col 8, lines 13-17 and Fig 5, internal bus 37).

Claim 3:

Easter further discloses wherein said digital secret is securely confined within said processor (col 8, lines 18-22).

Claim 5:

Easter does not explicitly disclose wherein said internal memory securely stores intermediate data created within said key-based cryptographic process. However, official notice is taken that having a software based DES engine and internal memory that securely stores intermediate data created within a key based cryptographic process was well known in the art at the time applicant's invention was made. It would have been obvious to one skilled in the art to modify Easter's DES engine to utilize software and to have the internal memory securely stores intermediate data created within said

Art Unit: 2135

key-based cryptographic process. One skilled would have been motivated to do utilize a software DES engine because it is a design choice and one skilled would have been motivated to have the internal memory securely store intermediate data created by the DES engine because it would prevent leaking of the DES key. The DES key is an intermediate data.

Claim 6:

As per the limitation that the processor of claim 1 further comprises a cryptographic unit comprising a functional unit within said processor for securely executing said key-based cryptographic process internally within said processor, wherein said cryptographic unit comprises: said digital secret; said cryptographic engine; and said internal memory, it is obvious to the combination invention of Easter and Chorley. Note that as discussed in claim 1, said digital secret; said cryptographic engine; and said internal memory are contained in Easter's integrated circuit 53 (Fig 5), which is meant for incorporation into circuitry (col 6, lines 14-15). If one were to incorporate integrated circuit 53 into Chorley's secure processor as intended by Easter, one would end up with a processor as recited in claim 6. Integrated circuitry 53 can be considered the recited cryptographic unit. Note also that making things separate or integral is obvious (see MPEP 2144.04(V)(B)).

Claims 7 and 11:

Easter further discloses wherein said key-based cryptographic process comprises: a key based encryption process; and a key-based decryption process (col 4, lines 27-29).

Claims 9 and 14:

Easter does not explicitly disclose wherein said digital secret is unique to said processor and is permanently and physically manifested within said processor.

However, official notice is taken that using a key unique to a processor was well known in the art at the time applicant's invention was made. It would have been obvious to one skilled in the art to utilize a digital secret that was unique to the processor because a DES key is meant to be secret and use of a unique key would prevent accidental access to the software being secured by Easter and Chorley's secure processor.

Further, Easter discloses that it was known to permanently and physically manifest a key within a processor (col 2, lines 44-46; col 5, lines 6-11; and col 8, lines 29-31). Storing of a key via a fuse array would permanently and physically manifest a key within the processor. At the time applicant's invention was made, it would have been obvious to one skilled in the art to further modify Easter and Chorley's combination invention such that the DES key was permanently and physically manifest a key within the processor. The rationale for why it is obvious is that the simple substitution of a key which is not permanently and physically manifested in the processor for one that is would do no more than yield a predictable result. One skilled would have been motivated to do so because it would ensure the secrecy of the key (col 8, lines 29-31).

Claim 15:

Easter does not explicitly disclose wherein said digital secret comprises a plurality of fusible links to manifest said digital secret by permanently setting a binary state in each of said plurality of fusible links. However, Easter discloses that it was

known in the art to use a plurality of fusible links to manifest a key by permanently setting a binary state in each of the plurality of fusible links (col 5, lines 10-11 and 26-47 and col 8, lines 29-31).

At the time applicant's invention was made, it would have been obvious to further modify Easter and Chorley's combination invention according to the limitations recited in claim 15 by programming a fuse array to store the DES key. The rationale for why it is obvious is that use of a fuse array to store the DES key instead of key array 25 is nothing more than the simple substitution of one known element for another to obtain the predictable result of a DES key stored in a fuse array. One skilled would have been motivated to do so because it would ensure the secrecy of the key (col 8, lines 29-31).

Claims 18 and 26:

As per the limitation that said secure cryptographic unit comprises a fully integrated circuit within said processor, it is obvious to the combination invention of Easter and Chorley. Easter's integrated circuit 53 is a fully integrated circuit (Fig 5) and is meant to be incorporated into a circuit (col 6, lines 14-15). When IC 53 is incorporated into Chorley's secure processor, it would be incorporated as a separate secure cryptographic unit, thus the limitation further recited in claim 18 is made obvious. Note also that making things separate or integral is obvious (see MPEP 2144.04(V)(B)).

Claim 19:

Easter further discloses wherein said digital secret and said internal memory are fully integrated with said cryptography engine to facilitate communication without use of a bus (Fig 5 and col 6, lines 14-15).

Note that the above limitation is interpreted as best understood from what is disclosed in the specification. The examiner assumes that “without use of a bus” refers to an external bus and does not refer to internal buses since one skilled in the art would recognize that any type of circuit would have some form of busses, thus the total absence of a bus in a circuit or processor is impossible. The cryptography engine, internal memory, and digital secret seen in Figure 5 of Easter is encapsulated as one unit (i.e. IC 53), thus these components do not utilize any external busses to communicate.

Claim 20:

Easter does not explicitly disclose wherein said key-based cryptography process comprises a Triple Data Encryption Algorithm (TDEA or Triple DES) cryptographic process. However, official notice is taken that Triple DES was a well known cryptographic process at the time applicant's invention was made. It would have been obvious to one skilled in the art to modify Easter's invention such that said key-based cryptography process comprises Triple DES cryptographic process. One skilled would have done so because Triple DES is more secure than DES. Further, it would have been obvious to do so because the substitution of a Triple DES engine for a DES engine would do no more than yield a predictable result.

Claim 4 is rejected under 35 U.S.C. 103(a) as obvious over Easter et al (US 5,563,950) in view of Chorley et al (US 4,634,807) in further view of Galasso (US 6,598,165) and Moyer et al (US 2004/0243823).

Claim 4:

Easter does not explicitly disclose wherein said internal memory comprises microcode for implementing said key based-based cryptographic process on data within said processor, and wherein said internal memory is operable to perform state tracking associated with said key-based cryptographic process.

However, Galasso discloses a key-based cryptographic process performed on data within a processor which utilizes microcode contained in an internal memory (col 3, lines 1-20). At the time applicant's invention was made, it would have been obvious to one skilled in the art to further modify Easter and Chorley's combination invention such that said internal memory comprises microcode for implementing said key based-based cryptographic process on data within said processor. The rationale for why this is obvious is that the simple substitution of the DES engine disclosed by Easter with a software based DES engine disclosed by Galasso, which requires the internal memory to comprise microcode for implementing the DES algorithm is nothing more than simple substitution of one known element for another to obtain predictable results.

Further, Moyer discloses internal memory operable to perform state tracking associated with a data processing system (paragraphs 12 and 14). Moyer's invention tracks the state of a data processing system to determine when errors or access violations may occur (paragraph 4). At the time applicant's invention was made, it

would have been obvious to further modify the combination invention of Easter, Chorley, and Galasso such that the internal memory is operable to perform state tracking associated with said key-based cryptographic process. One skilled would have been motivated to do so because it would improve the security (Moyer: paragraph 38) of the secure processor having the software DES engine by catching errors and access violations. Note that the DES engine is a data processing system.

Claims 8, 13, and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Easter et al (US 5,563,950) in view of Chorley et al (US 4,634,807) in further view of Fahrny (US 2004/0098591).

Claims 8, 13, and 22:

Easter further discloses a secure hardware environment providing core processing functionality (Fig 5).

Easter does not explicitly disclose secure software environment coupled to said secure hardware environment, said secure software environment generating executable instructions that are sent to said secure hardware environment for processing, said secure hardware environment in combination with said secure software environment providing processor capability, and wherein said secure hardware environment is accessible only through said secure software environment.

However, Fahrny discloses a secure software environment coupled to a secure hardware environment (paragraphs 10 and 26), said secure software environment generating executable instructions that are sent to said secure hardware environment for processing (Fig 1 and paragraphs 26-28), said secure hardware environment in combination with said secure software environment providing processor capability, and wherein said secure hardware environment is accessible only through said secure software environment (Fig 1, item 16 and paragraphs 28 and 31).

Note in the cited section of Fahrny that a secure hardware (Fig 1, item 16) authenticates software objects, including a trusted operating system at initialization. Access to any items in the secure hardware has to be done via an authenticated software object, i.e. trusted OS. The combination of authenticated software objects, i.e. secure software environment, along with the secure hardware (Fig 1, item 16) provides processor capability.

At the time applicant's invention was made, it would have been obvious to one of ordinary skill in the art to modify Easter and Chorley's combination invention according to the limitations recited in claim 8 in light of Fahrny's teachings. One skilled would have been motivated to do so because Fahrny's teachings would further protect data within a secure hardware, i.e. Easter and Chorley's secure processor, by authenticating software objects prior to allowing the software object access to any data in the secure hardware (Fahrny: paragraph 10). This would further ensure that unauthorized users could not access the software encrypted software or DES key illegally.

Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Easter et al (US 5,563,950) in view of Chorley et al (US 4,634,807) in further view of Cmelik et al (US 6,031,992).

Claim 12:

Easter does not explicitly disclose wherein said processor comprises a very long instruction word processor (VLIW) processor. However, Cmelik discloses wherein a processor comprises a very long instruction word processor (VLIW) processor (col 8, lines 51-65). At the time applicant's invention was made, it would have been obvious to one skilled in the art to further modify Easter's invention according to the limitations recited in claim 12 in light of Cmelik's teachings. One skilled would have been motivated to do so because use of a VLIW processor would increase the speed of processor execution (Cmelik: col 9, lines 51-65).

Claims 16-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Easter et al (US 5,563,950) in view of Chorley et al (US 4,634,807) in further view of Balard et al (US 2004/0025036).

Claim 16:

As per claim 16, Easter does not disclose wherein said digital secret comprises a random number that is generated from an HMAC algorithm implemented on testing data associated with fabrication of said IC chip. However, Balard discloses the limitation

(Figures 2 and 10). It would have been obvious to one skilled in the art to further modify Easter's invention according to the limitations recited in claim 16 in light of Balard's teachings. One skilled would have been motivated to do so because it would ensure uniqueness of the DES key.

Claim 17:

As per claim 17, Balard further discloses wherein said testing data comprises die test data (paragraph 42 and Fig 6). However, Easter, Chorley, and Balard do not explicitly disclose testing data comprising wafer test data. However, official notice is taken that testing data comprising wafer test data was well known in the art at the time applicant's invention was made. It would have been obvious for one of ordinary skill in the art to include wafer test data within the combination invention of Easter, Chorley, and Balard as said testing data because testing a processor's wafer ensures quality of the processor.

Claims 23, 24, and 26 are rejected under 35 U.S.C. 103(a) as obvious over Easter et al (US 5,563,950) in view of Chorley et al (US 4,634,807) in further view of Moyer et al (US 2004/0243823)

Claim 23:

Easter further discloses wherein said secure cryptography unit further comprises:

1. A cryptography engine for performing said key based cryptographic process (Fig 5, DES engine 21).

2. Said digital secret accessible exclusively to said cryptography engine , wherein said digital secret comprises a secret key used in said key-based cryptographic process (col 4, lines 28-29 and col 8, lines 10-22).
3. Internal memory coupled to said cryptography engine for supporting said key-based cryptographic process (Fig 5, items 25 and 37).

Easter does not explicitly disclose said internal memory performs state tracking associated with said key-based cryptographic process. However, software based DES engine were well known in the art. Further, Moyer discloses internal memory operable to perform state tracking associated with a data processing system (paragraphs 12 and 14). Moyer's invention tracks the state of a data processing system to determine when errors or access violations may occur (paragraph 4). At the time applicant's invention was made, it would have been obvious to further modify the combination invention of Easter and Chorley such that a software DES engine was used and the internal memory is operable to perform state tracking associated with said key-based cryptographic process. One skilled would have been motivated to use a software DES engine because use of a software or hardware DES engine is an obvious design choice. One skilled would have been motivated to incorporate Moyer's teachings in the manner discussed because it would improve the security (Moyer: paragraph 38) of the secure processor having the software DES engine by catching errors and access violations. Note that the DES engine is a data processing system.

Claim 24:

Claim 24 recites a further limitation substantially similar to what is recited in claim 5 and is rejected for similar reasons.

Claim 26:

Claim 26 recites a further limitation substantially similar to what is recited in claim 19 and is rejected for similar reasons.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to PONNOREAY PICH whose telephone number is (571)272-7962. The examiner can normally be reached on 9:00am-4:30pm Mon-Thurs.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2135

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Ponnoreay Pich/
Examiner, Art Unit 2135
/KimYen Vu/
Supervisory Patent Examiner, Art Unit 2135